NATIONAL MUSEUM OF THE UNITED STATES AIR FORCE

Cyber Security and Protection

Students will gain an understanding of cyber threats and a means of preventing them. Through the use of the game activity, they will recognize and know how to respond to these threats.

LEARNING OBJECTIVES:

- Students will be taught how to recognize cyber threats they might encounter while participating in a variety of online activities.
- They will use a number of tools and practices to protect themselves while online.
- They will apply this knowledge in a game designed to reinforce these preventative tool and methods to reduce their risk of cyber threats.

Grade Level: 6-8

National Science Education Standards:
Science and Technology, Understanding Technology.

Standards for Technological Literacy:
Technology and Society, Design, Abilities for a Technological World, and the Designed World.

GOAL:

Each hour of every day, the United States Air Force faces cyber threats to its multiple and varied cyber systems. These threats come from a variety of global antagonist. In order to grasp the depth and meaning of these threats, we must understand what some of these threats are, where and how they originate and how to protect against them. In this lesson, students will discuss their personal online experiences and learn how to reduce the would-be cyber risks that they may encounter while online.

Students will be provided a *Cyber Security Tip Sheet*, to determine which tools and strategies they can successfully use to eliminate or prevent damaging online experiences. Once they have gained and understanding of this information, students will test their knowledge by playing the *Cyber Protection Game.* In this activity, they will work in groups as they compete against other students to match cyber risks with the appropriate protective cyber tools.

Materials Required:
- *Cyber Security Tip* Sheet—Handout
- *Cyber Security Game*—Instructions
- One copy of the *Scenario* card deck– *cut out*
- Two copies of the *Risk* cards- *cut out.*
- Three copies of the *Tool- cut out*

All Handout Materials are Attached.

INTRODUCTION (Day One):

As our society and classrooms evolve to include more technology, it is important that we teach our students the threats they may encounter online and what tactics and tools they can use to protect themselves against these threats.

PROCEDURE (Day One)

Online Risks:

Start your lesson plan by asking students what they like to do online (ask what sites they visit, what games they download, where they shop, etc.) Note their responses on a chart, you've previously created, with three headings titled: *Talk, Shop and Play*. Sort the student's responses under these three headings.

Next, ask students about any negative experiences they may have had while online. Place their responses in one of the three categories mentioned above. In-depth discussion is not necessary. Students need not provide examples.

Ask students if they are aware of some of the risks they may encounter while online (again, students do not need to elaborate). Try to steer the conversation to include publicized risks such as interaction with strangers. Encourage students to explore ideas related to "bad-links" which redirect them to other sites and gaming interference.

Distribute the *Cyber Security Tip Sheet* and review it with students. Remind the students of their own online experiences, then read them the following scenario:

"You visit Booksandmorebooks.com to buy a book for a school report. When you leave that site, you decide to spend a few minutes playing your favorite game, *Shazamit.* Then you go to *Whatisit* to do a research before you leave on your family vacation to Europe. The next time you go online you begin to get ads for these new sites on all of your social network sites. How do these sites suddenly know so much about you?"

Ask your students what type of risk is being represented through this scenario. They will probably figure out quickly that "cookies" may have been installed on their computer system. Using the *Cyber Security Tip Sheets*, direct them to the "tools" section and discuss how each tool would help prevent "cookies" from tracking their online habits. Some suggestions are: updating virus software, clearing their browser history, using private browsing tools and using more secure sites.

Explain to your students that over the next few days they will identify risks and apply the appropriate tools to different scenarios using the "*Cyber Security Activity."*

At the close of class, ask students to review and become familiar with the *Cyber Security Tip Sheet* for the next day's class.

Day Two

Provide your students with the *Cyber Security Game* instructions and remind them that they are going to complete an activity that will teach them about potential cyber threats while they are online. The activity will give them tools to prevent these problems and provide solutions on how to fix them should the threats happen.

Divide the class into no more than 10 groups of two or three students.

Give each group one **Scenario** card and randomly pass out the **Risk** cards, only two cards per group. If there are remaining **Risk** cards hold onto them for Step 3 of the activity.

Give each group time to play the game. (This is dependent on the length of your class period).

1. First, group members need to identify the trade with other groups until they find the appropriate card that matches the "scenario."
2. If you have the **Risk** card they require, students may also trade with you, the teacher. They may not review your cards for their choice, but they must randomly select one from your deck.
3. Once they have the necessary **Risk** card, students will use the *Cyber Security Tip Sheet* to select two "tools" that can be used to prevent or repair that risk.
4. Students then tell you which **Tool** they would use on their **Risk** and why. They will use the *Cyber Security Tip Sheet* to determine if they have made the threat found in the **Scenario** cards. What is it?
5. If they do not have a related **Risk** card, they must right choice. If they have made the correct choice, students get to choose two **Tool** cards. The students must then acquire, by trading with you or others students, **Tool** cards matching the "tools" they have chosen to minimize or prevent their risk.

How to Win the Cyber Security Card Activity

The first group to complete all of the following tasks is the winner.

- Correctly identify the **Risk** in their Scenario
- Collect the **Risk** card from the other groups
- Correctly identify and use two relevant tools
- Acquire the appropriate **Tools** card

If you have time, you can ask the other groups to continue to play to determine second, third, fourth place and so on.

Students will be asked to share their findings with the class.

NOTE: This is intended to be a fast-paced, kinesthetic activity.

Example of play:

A group of three students receives a **Scenario** card and two **Risk** cards**.** The **Scenario** card reads, "You were in a hurry to check your *Eyelook* account this morning and you accidently typed in www.eyelock.com. Instead of going to *Eyelook*, you went to a site that sells eyeglasses."

A group of students correctly identifies the risk to them as cybersquatting, but the **Risk** card they received reads *"Griefing"* and "*Malware."* The group moves about the room going to other groups while attempting to find the group that has the "*Cybersquatting"* card. The group does not need either the "*Griefing*" or "*Malware*" cards, but they do need the "*Cookies"* card.

Once the group finds the group that has the "*Cookies*" card, they can trade their "*Griefing*" card for it and then they can trade their "*Cookies*" card with another group that has the "*Cybersquatting*" card.

Next, the group checks the *Cyber Security Tip Sheet* and identifies "*Bookmarks"* and "*Content Filters"* as tools that should be used to prevent cybersquatting.

The group shares their **Scenario** card and related **Risk** card with the teacher, If they have correctly identified the risk then they draw two **Tool** cards, one reads, "*Strong Passwords,*" the other reads "*Content Filters.*" The last card is the one the group needs but, they must also have the card that reads "*Bookmarks*." So the students go back to the other groups seeking that card.

The first group finds another group of students which have the "*Bookmark"* card while that group needs the "*Strong Passwords"* card, so the two groups trade. The first group takes their card and returns to the teacher. Because they've previously identified the risk in the **Scenario** card, identified the required tools to prevent the risk and they were successful in getting the needed **Risk** and **Tools** cards, they win.

Designing a Cyber Security Activity for Grades 7-8

Students will be asked to create their own "cyber" board activity. In order for them to do this, they must understand the components of one. This one can be done by teaching students about board game design. Ask students to name a few of their favorite board games. Once they have done so, pass out the "*What is a Board Game?"* worksheet, and review it with them. Collectively, select a game which everyone is familiar and analyze it using the handout content sheet. For example, the game *Monopoly*® might be evaluated as such:

A Goal — To be the wealthiest player.

A Way to Win — Bankrupt the other players and collect the most assets. Be the only player with money left.

Competition — Players are competing against each other. There are in-game obstacles that present challenges along the way.

Chance — A roll of the dice determines where you will move and land on the board. *Chance*® and *Community Chest*® cards also impact the players chance to gain or lose money or position on the board.

Playing Pieces — All players have one game piece and they are removed from the board only when a player has lost.

Board Design — In *Monopoly*®, the playing board is designed to represent a city with different streets and locations of that city. These locations represent various socio-economic classes based on divisions of wealth and the ability to purchase utilities. There are also bonuses and traps, for instances passing, "Go" or going "Directly to Jail." Additionally, properties purchased and developed by other players can present a financial "trap" as they require "rent" to be paid when landed upon.

Once the "*What is a Board Game?"* sheet is discussed, divide the class into 4-6 groups and hand out the "*Board Game Analysis Worksheet."* Have each group select a second board game and analyze it using the worksheet. Once finished, the groups should be ready to present their findings to the class.

Now that the students have an understanding of the purpose and design of board games, groups will create their own. Using the "*Designing a Cybersecurity Board Game"* worksheet as a guide. Group board games should be based on the content of the *Cybersecurity Tip Sheet*, and players must have a thorough understanding of this content in order to win the game. Students can be given the opportunity to play their own and each others games to determine effectiveness.

CYBER SECURITY TIPS

Most of the activities we perform online fall into one of three categories: *Talk, Shop* and *Play*. Each category has its own risks of which we should be aware so that we can protect ourselves and our computer equipment. Below are some examples of risks encountered while online and tools you can use to avoid them.

Risks:

Cybersquatting — This risk involves sites designed to look identical to another, often, more popular site. The web address for each site is very similar to the other and can sometimes be typed by mistake. These imposture sites are designed to steal user information and money.

Tools for this type of threat include: Bookmarks and Content Filters.

Cookies — Cookies are smaller files that are unknowingly saved to your browser through a website you have visited. These files are designed to capture your email, passwords and can track your online activity. These files can live in your system for months.

Tools to prevent cookies: Installing browser and antivirus updates, increasing privacy settings and using secure sites to transfer most personal data.

Data Theft — Online thieves can do major damage to your personal and financial accounts if allowed access.

Tools for preventing financial and identify theft include: Using book marks often visited, valid sites, blocking other users with whom you are unfamiliar, updating browsers and antivirus software, creating strong passwords, encrypting emails, turning on firewalls and privacy settings, using secure sites.

Overspending — Often, using money online can cause us to loose track of amounts spent. This can be financially damaging.

Tools to prevent overspending online include :Using pre-paid credit cards, logging online spending.

Griefing — These folks are also referred to as "trolls". They are the bullies of the online world and will make statements simply to provoke, antagonize or irritate.

Tools for "trolls" include: Blocking those users, contacting the content administrator for the site where the "troll" resides, and increasing your security settings.

Identity spoofing — Online anyone can be you and you can be anyone. In the dating world this idea would be similar to "catfishing". A person claiming the identify of another so that they appear to be more perfect in some or many aspects.

Tools to reduce identity spoofing can include: Email encryption, turning on firewalls, managing your reputation online.

Identity Theft — Your online identity can include a vast amount of personal and financial information. If not protected, an online thief or scammers can have access to all of it.

> *Tools to minimize the risk of identity theft include: Updating antivirus software, encrypting emails, turning on firewalls and turning up privacy protections and using only secure sites to transmit personal and financial information.*

Malware — These malicious codes are often hidden in useful or authentic programs. They can be installed through gaming sites or other popular sites. These viruses, worms and Trojan horses harm your computer system and the files contained within it.

> *Tools to protect yourself from malware include: Using bookmarks, installing antivirus software, and turning on firewalls.*

Online Fraud — Because we don't know for certain who we are dealing with while online, it is often easy to get scammed by a person or fake company.

> *Tools to prevent online fraud can include: Contacting the site administrator, using pre-paid credit cards, using only secure sites to shop (https).*

Phishing Scams — Phishing scams will use authentic looking email, sites, forms and questions in an effort to get you to disclose personal and financial information.

> *Tools to prevent phishing include: Email encryption, reporting phishing to the site administrator and using secure sites.*

Spyware — This type of software is delivered via authentic websites. It can track your web movement and collect personal information about you.

> *Tools to limit spyware can include: Using bookmarks, setting firewalls and installing anti-virus software.*

Tools:

Now that students know some of the risks, discuss the tools that have been suggested to prevent, correct or minimize the threats to them.

Bookmarks — By clicking at the top of your web browser page, you can save your trusted or most used websites under your "favorites."

Blocking other Users — Students can block others from seeing or sharing your data on almost every type of data transport system such as: websites, text, email and phone.

Browsers and Anti-virus updates — Your browser is your first line of defense to protect from online intrusion. Keep the latest version installed. Do the same with your anti-virus software.

Cleaning your browser cache — Cleaning up after yourself prevents others from finding what you've left behind. Sometimes, a trail of crumbs can lead to a "cookie."

Contacting sites and ISPs (Internet Service Provider) — Don't hesitate to report bad or suspicious behavior to a website's administrator or ISP host.

Content Filters — Using browsers, ISPs, specific websites and software are all ways to control unwanted content.

Creating strong passwords — Use passwords that are AT LEAST seven characters and have upper and lower case letters, with numbers and special characters. Don't use often applied passwords like, "1,2,3,4" or 'password." These passwords are easily guessed and can allow your information to be compromised.

Email encryption — Some email services provide for encryption. There is also software to prevent the interception and reading of your emails.

Firewalls — These protections prevent unauthorized access into your computer and it's components.

Managing reputation — Always keep in mind that others can see you, your pictures and your posts, especially on social media sites. To manage this content, do a web search for your name. If you see unfaltering content ask the ISP that it be removed.

Prepaid credit cards — These can be purchased at any grocery or big package store. These can help limit what you spend online.

Privacy policies — Any site collecting your information should have a privacy setting and should be clear about that policy. If this is not the case, do not visit the site and certainly do not give them information.

Privacy settings — These settings let you decide who sees your information. The default settings are not the most secure, so take time to review them and set them to a level which protects your data.

Reporting online crime — Online crime can only be stopped if the proper persons are made aware. At school, contact your teacher and IT staff. At home, contact the web administrators, ISPs and if needed, the local law enforcement authorities.

Secure Sites — These websites have established encrypted settings to protect users. They can be identified through their "https" URL address.

User/vendor rating system — Some websites allow users to rate a website on their experience while there. Review these ratings to finding any reports of scamming, phishing or disruptive behavior experienced by other visitors.

Cyber Security Activity Scenarios (Teacher Answer Key):

Scenarios 1-10 will match the back of the **Scenario** cards**.**

1.) You were in a hurry to check your *Eyelook* account and accidentally typed www.eeylook.com instead of eyelook.com. Instead of going to *Eyelook* you landed on a page that sells designer glasses

Risk: Cybersquatting
Tools: Use bookmarks and content filters

2.) Recently, you bought a book at booksandmorebooks.com using your *Payup* account. Today you found out that your account had been used to buy thousands of dollars of other items at that website.

Risk: Data Theft
Tools: Block other users, update browser and antivirus software, cleanout browser history, create strong passwords, use email encryption, bookmarks and firewalls, increase privacy settings, use private browsing tools, report online crimes, shop only on secure sites.

3.) You were shopping at booksandmorebooks.com and found a number of books that you wanted to read. Today, you found that in your excitement you had spent over $200.00.

Risk: Excessive spending
Tools: Use pre-paid credit cards, install content filters.

4.) *Shazamit* is the hottest game with your friends so you decide to try it. Every time you log into the game, you are defeated by a more skilled player and they take all your winnings. You try to keep playing, but the same player keeps defeating you every time you log back into the game.

Risk: Griefing
Tools: Block other users, contact the site and ISPs, increase content filters and privacy settings, provide reviews at the vendor/user rating system.

5.) At school today, your best friend was very upset with you. When you asked why, she said, "I didn't like what you wrote about me on *Eyelook* — but you didn't write those things.

Risk: Identity spoofing
Tools: Block other users to your accounts, update browsers and anti-virus protection, encrypt emails, turning on firewalls and increase privacy settings.

6.) Yesterday you received a bill from a credit card agency for $500.00. You don't have a card with that group. Someone used your name, address and other information to open a fake account.

Risk: Identity Theft
Tools: Use bookmarks, update browser and anti-virus protection, clean out browser history, turn on firewalls, and increase security settings, report online crimes.

7.) For the last month your computer has been getting slower, yesterday it froze and refused to re-boot. You took it for tech service and found that it had several viruses.

Risk: Malware
Tools: Use bookmarks, browser and virus protection updates, secure sites and turn on firewalls.

8.) You received an email from *Payup*, stating that your account information was out of date. After you sent your information, someone used your account to buy a large number of items.

Risk: Phishing
Tools: Encrypt emails, report online crime.

9.) You bought a skateboard from a person on *Sportlist* and you paid using your *Payup* account. You never received the board. You sent an email to the seller, but haven't heard anything back.

Risk: Online fraud
Tools: Use bookmarks, contact the sites and ISPs, use prepaid credit cards, use secure sites, report online crime.

10.) While trying to log into your *Eyelook* account you found that someone had changed the password. You found that all of your passwords for online accounts had been changed. You took your computer for IT support and they found that someone had installed a program that allowed them to watch your online activities.

Risk: Spyware
Tools: Use bookmarks, install browser and virus updates, turn on firewalls and use secure sites.

BEGIN LESSON PLAN

Cyber Security Activity Student Handouts):

What is a Board Game?

People have been playing board games for more than 4,000 years. The oldest that is known was *Senet*, and it was played by Egyptians. Today, there are numerous board games available, and despite the difference they all have some things in common. It is these similarities that you must keep in mind while designing your own game.

After learning about these similarities, you will be asked to design your own game that will test players' knowledge and understanding of the **Risks** and **Tools** described in the *Cyber Security Tip Sheet*.

Goal: To be considered a game, there must be some type of anticipated outcome. The players must be trying to reach the goal set out for them. There are typically four types of goals in board games. Some games can combined two or more anticipated goals.

Race — Players are competing to be the "first" to achieve a set goal or to get to a certain point on the board. Games such as *Candyland*® and *Shoots and Ladders*® are considered to be a fast-paced "race" style game.

Collecting — Players are competing to get the most of a resource or item. *Monopoly*® and *Trivial Pursuit*® are examples of this game type.

Defeating the Enemy — Players are trying to win a "battle" against the other player(s). *Rockem Sockem Robots*®, *Checkers*® and *Hungry, Hungry Hippo*® are examples of these battle games.

Building — The goal with these games is for players to build or secure an item or structure. *Jenga*® and *Othello*® fall into this type of game category.

A Way to Win: Once a game's goal is set, the means to achieve that goal needs to be established. This should determines how the player(s) will win.

First player to reach a certain point —The player who reaches the established points first, wins. For example, in *Trivial Pursuit*®, the first player to gain all the topic wedges and reach the center of the board, wins.

Last person standing — The last person to be eliminated from play. In *Monopoly*®, the winner is the person who has a majority of the money and property.

Limited or no remaining resources — All of the game resources have been used or it is not possible for any player to make additional moves. In *Chess*, this can be shown when the King cannot make any legal moves and a stalemate must be declared. It can also be shown in *Apples to Apples*® or *Dominoes*® when all the cards or tiles have been used.

Time limit — The game ends after a set period of play. The winner is decided by which player has more resources or a better position on the board. In the game *Perfection*® , there is a timer built into the game to limit the time. When time runs out, the pieces pop up and out of the game board. The player with the least number of game pieces is declared the winner.

Competition: In order to make a game more challenging, there needs to be obstacles within the game.

Obstacles — These "traps" make it more difficult to win.
In *Monopoly*® , "Going to Jail", slows the progress of other players.

Other Players — In most games, there is direct competition against other players. Often, there are ways for the players to make progress and winning more difficult for others.
Once again, *Monopoly*® allows for those players who have gained more property the opportunity to collect "rent" from other plays, making it more difficult for those players to save their money and win.

Chance: With the exception of some strategy games, most games have a random opportunity of "chance." The concept of "chance" can be achieved through the roll of the dice, a card draw, a spinner or other methods. There are many things in the game that can be impacted by chance, such as; advancing forward or back, gaining "prizes" and ultimately, winning.

Moving — Chance can decide how far a players' piece moves on the game board.

Fighting — Chance can also determine who wins a battle. For instance, if players are trying to determine who goes first they may roll the dice. The player who rolls the highest number, wins.

Resources — Chance can also determine who gets what resources in a game.

Pieces: In all board games, there are pieces for each player to play with. These pieces can change from game to game.

Number — Players will get a set number of playing pieces.

Type — In some games, pieces simply represent the players. In other games, the pieces serve a specific purpose and can be used in different ways. In *Chess*, each piece on the board has a certain position and role which dictate the movement of each piece on the board.

Permanence — Some games will allow pieces to be removed from the board by either player. This can be a result or strategy or a process of winning. Examples again include, *Chess* and *Checkers*.

Board: The game board is where the game takes place. The shape and spaces on the board must be considered when designing the game board.

Shape: There are four basic shapes traditionally used in game boards.

Line—This is the most common shape. The game *Clue*® follows this pattern.

Circuit—Players follow a loop design during game play. This design can be seen on a *Trivial Pursuit*® board.

Grid—The board has both vertical and horizontal squares, sometimes of equal number. This is most often seen in strategy games. Good examples of this type of game board are *Battleship*® and *Connect Four*®.

Map —The board is created to show territories or a specific space. This type of board can be seen in *Risk*® and *Monopoly*®.

Special Spaces: Many game boards have special spaces that can influence play. These spaces can benefit or hinder players.

Traps — Land on these spaces and you may "move back two spaces" or "loss a turn."

Shortcuts — Land here and you can move forward.

Bonuses—These spaces will provide rewards that will help you toward your goal.

Random — These spaces can provide players with either benefit or harm to their goal.

Forks — Landing on these spaces will give the player the chance to choose their options or movements.

Analyzing a Board Game

Discuss a board game that you like to play.

1. What is the goal of the game?

_____

_____

_____

2. How do players win the game?

_____

_____

_____

3. What sort of competition do players encounter?

_____

_____

_____

4. Does "chance" play a role in the game? If so, what sort?

_____

_____

_____

5. Are there game pieces? Does everyone get the same number, with the same role and rules?

_____

_____

_____

Board Game Design Worksheet

Using the information you've gained in class, create a game board using the **Risks** and **Tools** in the *Cyber Security Tip Sheet.* Design your game so that knowing the **Risks** and **Tools** are rewarded in the game. Players should not be able to win without knowing this information.

Design your game by answering each question below. For each question, consider how you can make the **Risks** and **Tools** a part of the game. Once the concept is determined, create your game board. Include game pieces, cards, random elements, etc. Once you have all of these considerations, create the rules for play.

1. What is the goal of your game? Consider how the **Risks** and **Tools** relate to these goals.

   _____

   _____

2. How many players can play your game at one time?

   _____

   _____

3. How do players win? How do the **Risk** and **Tools** you've learned relate?

   _____

   _____

4. Do players compete against the game or other players?

   _____

   _____

5. What role does "chance" play in this game?

   _____

   _____

6. How many pieces does each player receive?

_____

_____

7. Do the pieces play different roles in the game? Are there multiple playing pieces?

_____

_____

8. What does the board look like? What is the shape? What are the special spaces on the board and what roles do those spaces play?

_____

_____

_____

_____

Student Evaluation Rubric

	Excellent	Good	Satisfactory	Needs Improvement
Knowledge/ Understanding	Game clearly demonstrates an awareness and understanding of all risks related to online security and the strategies and tools used to stay safe online.	Game clearly demonstrates an awareness and understanding of most risks relating to online security and strategies and tools used to stay safe online.	Game demonstrates an awareness and understanding of many risks relating to online security and strategies and tools used to stay safe online.	Game did not demonstrate an awareness or understanding of many risks relating to online security and strategies and/ or appropriate tools and strategies to stay safe online.
Playability of Game	The goals, objectives and rules for the game were clearly communicated and all players understood what they needed to do to win.	The goals, objectives and rules for the game were fairly clear and all players understood what they needed to do to win.	The goals, objectives and rules for the game were clear with additional explanation. Some players had difficulty playing.	The goals, objectives and rules for the game were not clearly communicated and all players had difficulty playing.
Design	Game effectively used many elements discussed on *Game Design Worksheet*.	Game effectively used some elements discussed on *Game Design Worksheet*.	A few of the elements discussed on *Game Design Worksheet* were used in the game design.	Not many elements discussed on *Game Design Worksheet* were used in the game design.
Creativity	The game design showed considerable thought, creativity and was fun to play.	The game design showed good effort to make it fun to play. It incorporated creative elements.	Effort was made to make the game fun and interesting. Some elements made the game harder to understand. Little creativity shown.	Little thought shown in design. Game was not interesting or fun. Lack of creativity.
Polish	Varied materials in construction. Game is visually appealing.	Various color and at least 1 original graphic created for game board.	Various colors and existing graphics taken from other sources. Little visual appeal.	Little color and few graphics.

	**Scenario Cards** Describe a situation relating to doing something online.
	**Risk Cards** Have the names of types of risks that you can come across when you do things online.
	**Tool Cards** Have the names of tools you can use to prevent online risks.